UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF PENNSYLVANIA

IAN WERKMEISTER, individually and on behalf of others similarly situated, Plaintiff, vs. WAYNE BANK, Defendant.	Case No. **COMPLAINT—CLASS ACTION** **DEMAND FOR JURY TRIAL**

Plaintiff, Ian Werkmeister ("Plaintiff"), brings this Class Action Complaint ("Complaint") against Defendant Wayne Bank ("Wayne Bank" or "Defendant") individually and on behalf of all others similarly situated, and alleges, upon personal knowledge as to his own actions and his counsels' investigation, and upon information and belief as to all other matters, as follows:

I. NATURE OF ACTION

1. This action arises out of Defendant's failures to safeguard the confidential Personally Identifying Information[1] ("PII") of its customers, including Plaintiff and the proposed Class Members, resulting in the unauthorized disclosure of that PII in a cyberattack in May 2023 (the "Data Breach") to Wayne Bank's vendor, MOVEit.[2] The PII disclosed in the Data Breach

[1] The Federal Trade Commission defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8).

[2] *See, e.g.,* Wayne Bank Vendor Data Breach – MOVEit Event Notice, December 29, 2023 (hereinafter "Data Breach Notice") **attached as Exhibit A**. Available at https://wayne.bank/moveit-event/ (last accessed Feb. 9, 2024).

included Plaintiff and Class Members' names, dates of birth, Social Security Numbers (full), account numbers (full) and routing numbers/ABA numbers.[3]

2. Defendant Wayne Bank is headquartered in Honesdale, Pennsylvania.[4] Wayne Bank provides financial services including banking services and loan services to consumers and business.

3. As a condition of providing financial services, Wayne Bank required its customers to provide it with their PII, including names, dates of birth, and social security numbers.

4. Wayne Bank engaged a third-party vendor, an IT services provider, who in turn utilized MOVEit for its file transfer software and services.[5]

5. Unbeknownst to Plaintiff and the proposed Class Members, Defendant provided Plaintiff and Class Members' PII to MOVEit.

6. Wayne Bank failed to undertake adequate measures to ensure that MOVEit safeguarded the PII of Plaintiff and the proposed Class Members, including failing to ensure that MOVEit implemented industry standards for data security, and properly trained employees on cybersecurity protocols, resulting in the Data Breach.

7. Although Wayne Bank discovered the Data Breach on or about October 19, 2023, Defendant failed to promptly notify and warn Data Breach victims of the unauthorized disclosure of their PII for over two months, preventing them from taking necessary steps to protect themselves from injury and harm.

---

[3] See **Exhibit B**, copy of Data Breach Notice Letter received by Plaintiff, dated December 20, 2023.
[4] https://www.Wayne Bank.com/ (last visited Feb. 9, 2024).
[5] **Exhibit A.**

8. As a direct and proximate result of Defendant's failures to protect Plaintiff's and the Class Members' sensitive PII and warn them promptly and fully about the Data Breach, Plaintiff and the proposed Class have suffered widespread injury and damages necessitating Plaintiff seeking relief on a class wide basis.

II. PARTIES

9. Plaintiff, Ian Werkmeister, is a natural person and citizen of New York. He resides in Pine Bush, New York, where he intends to remain. And now, Plaintiff is a victim of Defendant's Data Breach.

10. Defendant, Wayne Bank, is a Pennsylvania financial institution with its principal headquarters located at 717 Main Street, Honesdale, Pennsylvania, 18431.

III. JURISDICTION AND VENUE

11. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Plaintiff and Defendant are citizens of different states. And there are over 100 putative Class Members.

12. This Court has jurisdiction over Defendant because it is headquartered in Pennsylvania, regularly conducts business in Pennsylvania, and has sufficient minimum contacts in Pennsylvania.

13. Venue is proper in this Court under 28 U.S.C. § 1391(b) because Defendant's principal office is in this District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

IV. BACKGROUND FACTS

Defendant Wayne Bank

14. Defendant Wayne Bank, headquartered in Honesdale, Pennsylvania, provides financial services including banking services and loan services to consumers and business.

15. As a condition of receiving financial services from Wayne Bank, Defendant requires its customers to provide it with their private, sensitive, PII, including their including their names, Social Security numbers, and dates of birth, which it stores in its information technology systems, and which it provides its third-party vendors, including MOVEit.

16. In collecting and maintaining PII, Defendant agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiff and Class members themselves took reasonable steps to secure their PII.

17. Wayne Bank acknowledges the importance of maintaining the security of its customers' PII it collects, stating to Data Breach victims that "Wayne Bank takes the protection of [its] customers' personal information very seriously[.]"[6]

18. In fact, Wayne Bank maintains a Privacy Policy ("Privacy Policy") (attached as **Exhibit C**) that is posted on its website.[7] In its Privacy Policy, Wayne Bank promises its customers that "it "works to ensure all customer information is protected" and that "customer privacy is one of [Wayne Bank's] top priorities." *Id*. The Privacy Policy further enumerates the following "[b]asic methods used to protect personal information within [Wayne Bank's] website":

> 1. Industry standard SSL encryption which protects customer information while it is being passed between bank systems and a client's browser.
>
> 2. The bank's processing center has very strict security with access to customer records limited to qualified staff only. The premises are continuously monitored; qualified personnel enter and exit via an electronically controlled locking system. All entrances and exits are recorded electronically.
>
> 3. Access to electronic data files requires multiple levels of authentication. All sensitive data, such as customer account numbers, remains encrypted at all times.

[6] Ex. A.
[7] https://wayne.bank/privacy-policy/ (last accessed Feb. 9, 2024).

4. Bank employees and its service providers' employees are aware of all security policies, procedures and practices. They give a pledge, in writing, to abide by a strict code of conduct.

5. All external system access to the bank's internal network must go through computer firewalls. Firewalls also protect application systems and stored data. The firewalls are regularly tested by highly qualified third parties to verify their ability to shield customers' personal data against unauthorized access of any type.

6. The bank and its data services provider utilize intrusion detection systems to continuously monitor and report unauthorized data access attempts.

Ex. C, Privacy Policy.

19. The Privacy Policy further represents to customers that, while Wayne Bank uses outside vendors to obtain services or provide specialized products to customers, the vendors are "contractually bound to safeguard [private customer information] and comply with the regulations and policies governing the bank." *Id.*

20. Despite the foregoing, Wayne Bank provided its customers' PII, including that of Plaintiff and the proposed Class, to its third-party vendor, which was then stored in its vendors' systems, without Wayne Bank ensuring that the vendor adequately safeguarded Wayne Bank's customers' PII.

21. Despite recognizing its duty to do so, on information and belief, Wayne Bank did not ensure that its vendor implemented reasonably cybersecurity safeguards or policies to protect its consumers' PII or supervised its information technology or data security agents and employees to prevent, detect, and stop breaches of its systems. As a result, there were significant vulnerabilities in the systems used to systems for cybercriminals to exploit and gain access to consumers' PII, resulting in the Data Breach.

22. In addition, Wayne Bank, by and through its agents and employees, represented to its customers, Plaintiff and the proposed Class Members, that Defendant would adequately protect their PII and not disclose said information other than as authorized, including as set forth in its Privacy Policy.

23. Plaintiff and the proposed Class Members, current and former customers of Wayne Bank, would not have entrusted their PII to Defendant in the absence of its promises to safeguard that information, including as set forth in its Privacy Policy.

24. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and the proposed Class Members' PII, Defendant assumed legal and equitable duties to Plaintiff, and the members of the Proposed Class, and knew or should have known that it was responsible for protecting his and their PII from unauthorized disclosure.

25. At all times Plaintiff and the members of the proposed Class, have taken reasonable steps to maintain the confidentiality of their PII; and, Plaintiff and the proposed Class Members, as current and former customers of Wayne Bank, relied on Defendant to keep their PII confidential and securely maintained.

A. The Data Breach

26. Plaintiff and the proposed Class Members are customers of Defendant, Wayne Bank.

27. As a condition of providing financial services, Defendant collected the PII of its customers, Plaintiff and the proposed Class Members, including but not limited to their names, addresses, dates of birth, and Social Security numbers.

28. In collecting and maintaining PII, Defendant implicitly agrees that it will safeguard the data using reasonable means according to industry standards, its internal policies, as well as

state and federal law. This duty extends to Wayne Bank entrustment customers' PII to its third-party vendors.

29. Defendant provided Plaintiff's and the Class Members' PII to its third-party vendor, MOVEit, who Wayne Bank uses as a secure file-transfer tool.[8]

30. On or about May 27, 2023, the PII of Plaintiff and the proposed Class Members which was entrusted to Wayne Bank was unauthorizedly disclosed to cybercriminals in the Data Breach, a Clop ransomware or external system breach attack impacting the MOVEit Transfer tool and the PII stored within.

31. According to Wayne Bank, as stated in the Data Breach Notice:

> On October 19, 2023, Wayne Bank was notified by a third-party Information Technology (IT) service provider of a data security incident that involved unauthorized access to a number of its financial institution clients' customer data, including Wayne Bank customer information, in one of their file transfer applications, MOVEit. Please note, the vulnerability discovered in MOVEit did not involve any of Wayne Bank's internal systems and did not impact our ability to service our customer.
>
> The incident involved vulnerabilities discovered in MOVEit Transfer, a file transfer software used by our vendor to support services it provides to Wayne Bank and its related institutions. MOVEit is a commonly used secure Managed File Transfer (MFT) software, which supports file transfer activities used by thousands of organizations around the world, including government agencies and major financial firms.
>
> Our service provider launched an investigation into the nature and scope of the MOVEit vulnerability's impact on its systems and discovered that the unauthorized activity in the MOVEit Transfer environment occurred between May 27 and 31, 2023, which was before the existence of this vulnerability was publicly disclosed. During that time, unauthorized actors obtained our vendor files transferred by MOVEit. These files included Wayne Bank and related institution customer information.

Ex. A.

[8] Data Breach Notice, Exhibit A.

32. Further, according to Wayne Bank, upon learning of the incident, Wayne Bank launched an investigation and began "notifying impacted customers." *Id.*

33. In reality, the Data Breach was executed by the notorious Clop ransomware gang, which claimed responsibility for the cyberattack, exploiting the MOVEit Transfer and MOVEit Cloud vulnerability for nefarious purposes and exfiltrating Plaintiff's and the proposed Class Members' PII. Clop is one of the most active ransomware actors, having breached over 2,000 organizations directly or indirectly in the MOVEit Transfer tool or cloud cyberattacks.[9]

34. Wayne Bank, a sophisticated financial services provider, knew or should have known of the tactics that groups like Clop employ.

35. Beginning on or around December 20, 2023, Wayne Bank began notifying its customers of the Data Breach by letter, the Data Breach Notice.[10]

36. Regarding steps Wayne Bank had taken in response to the Data Breach, Wayne Bank stated it enlisted a service provider to perform an investigation, and:

> Our service provider advises us that they have remediated the technical vulnerabilities and patched the systems in accordance with the MOVEit software provider's guidelines. To help prevent something like this from happening again, our service provider also mobilized a technical response team to examine the relevant MOVEit Transfer systems and ensure that there were no further vulnerabilities.

37. In its Data Breach Notice, Wayne Bank recognized the significant harm caused by the Data Breach. Wayne Bank advised the Data Breach victims to "remain vigilant and regularly review and monitor all of your credit history to guard against any unauthorized transactions or activity." Ex. B. Wayne Bank also recommended customers "closely monitor [their] bank account

[9] "Matthew J. Schwartz, Bankinfosecurity.com, "Data Breach Toll Tied to Clop Group's MOVEit Attack Surges," Sept. 25, 2023, avail. at https://www.bankinfosecurity.com/data-breach-toll-tied-to-clop-groups-moveit-attacks-surges-a-23153 (last acc. Dec. 12, 2023).

[10] See Exhibits A and B.

statements and notify us or any of your other financial institutions if [they] suspect unauthorized activity." *Id.*

38. Furthermore, Wayne Bank offered Data Breach victims two years of complimentary credit monitoring and identity restoration services through Kroll.[11]

39. Despite its duties and alleged commitments to safeguard PII, Defendant did not in fact follow industry standard practices in securing consumers' PII and ensuring that its vendor properly secured customers' PII, as evidenced by the Data Breach.

40. Wayne Bank failed to adequately protect the PII of its current and former customers, Plaintiff and the proposed Class Members, stored in its networks and which Wayne Bank gave to MOVEit, resulting in the Data Breach.

41. Wayne Bank failed to ensure that its vendor, MOVEit, employed adequate cybersecurity measures and adequately trained its employees on reasonable cybersecurity protocols to protect Wayne Bank's customers' PII, causing the PII of Plaintiff and the proposed Class Members to be unauthorizedly disclosed in the Data Breach.

42. As a result of the Data Breach, its victims face a lifetime risk of identity theft, as it includes sensitive information that cannot be changed, like their dates of birth and Social Security numbers. Accordingly, any credit monitoring and identity theft protection which Wayne Bank may offer is wholly insufficient to compensate Plaintiff and the Class Members for their damages resulting therefrom.

43. Indeed, as a result of the Data Breach which Defendant permitted to occur by virtue of its inadequate data security practices, Plaintiff and the proposed Class Members have suffered injury and damages, as set forth herein.

[11] *Id*.

B. The Data Breach was a Foreseeable Risk of which Defendant was on Notice.

44. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the file-transfer software industry preceding the date of the breach, including recent similar attacks against secure file transfer companies like Accellion and Fortra carried out by the same Russian cyber gang, Clop.[12]

45. In light of recent high profile data breaches at other file-transfer software companies, Defendant knew or should have known that its electronic records and consumers' PII would be targeted by cybercriminals.

46. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[13] The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[14]

47. Indeed, cyberattacks have become increasingly common for over ten years, with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime." [15]

---

[12] See https://www.bleepingcomputer.com/news/security/global-accellion-data-breaches-linked-to-clop-ransomwaregang/ (last visited on June 21, 2023); see also https://www.bleepingcomputer.com/news/security/fortra-sharesfindings-on-goanywhere-mft-zero-day-attacks/ (last visited on June 21, 2023).

[13] 2021 Data Breach Annual Report, ITRC, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf (last visited June 13, 2023).

[14] *Id*.

[15] Gordon M. Snow Statement, FBI https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector (last visited June 13, 2023).

48. Therefore, the increase in such attacks, and the attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Wayne Bank.

C. Plaintiff Ian Werkmeister's Experience

49. Plaintiff is a banking customer of Wayne Bank.

50. Plaintiff was notified by Wayne Bank of the Data Breach by letter, which he received on or around February 7, 2024.

51. Plaintiff entrusted his PII to Wayne Bank as a condition of receiving financial services, including but not limited to his name, date of birth, address, and Social Security Number.

52. On information and belief, Wayne Bank utilized MOVEit as a third-party vendor, and entrusted it with Plaintiff's and Class Members' valuable PII, which was stored in MOVEit's systems.

53. As a direct and proximate result of the Data Breach, Plaintiff has suffered, and imminently will suffer, injury-in-fact and damages.

54. As a result of the Data Breach, Plaintiff has and will spend time dealing with the consequences of the Data Breach, which will include time spent verifying the legitimacy of the Notice of Data Breach, self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred.. This time has been lost forever and cannot be recaptured.

55. In December 2023, Plaintiff began receiving scam phishing text messages purporting to be UPS.

56. Plaintiff has experienced feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or

inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

57. Plaintiff suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PII—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

58. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of unauthorized third parties and possibly criminals.

59. Plaintiff has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

D. Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

60. Plaintiff and members of the proposed Class have suffered injury from the misuse of their PII that can be directly traced to Defendant.

61. As a result of Defendant's failure to prevent the Data Breach, Plaintiff and the proposed Class Members have suffered and will continue to suffer damages, including unauthorized disclosure of this PII onto the Dark Web, monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a) The loss of the opportunity to control how their PII is used;

b) The diminution in value of their PII;

c) The compromise and continuing publication of their PII;

d) Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e) Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f) Delay in receipt of tax refund monies;

g) Unauthorized use of stolen PII; and

h) The continued risk to their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PII in its possession.

62. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.

63. The value of Plaintiff's and the Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen PII openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

64. It can take victims years to spot identity theft, giving criminals plenty of time to use that information for cash.

65. One such example of criminals using PII for profit is the development of "Fullz" packages.

66. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and

degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

67. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and the Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

68. Defendant disclosed the PII of Plaintiff and the Class to its vendor, MOVEit, who failed to take adequate measures to safeguard that PII, which was unauthorizedly disclosed in the Data Breach for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiff and the Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

69. Defendant's failure to promptly notify Plaintiff and members of the Class of the Data Breach exacerbated Plaintiff's and the Class's injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

E. Defendant failed to adhere to FTC guidelines.

70. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

71. In 2016, the FTC updated its publication, *Protecting Private Information: A Guide for Business*, which establishes cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of Private Information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[16]

72. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[17]

[16] *See* Federal Trade Commission, October 2016, "Protecting Private information: A Guide for Business," available at https://www.bulkorder.ftc.gov/system/files/publications/2_9-00006_716a_protectingpersinfo-508.pdf (last acc. Apr. 14, 2023).
[17] *See id*.

73. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

74. These FTC enforcement actions include actions against entities failing to safeguard Private Information such as Defendant. *See, e.g., In the Matter of LabMD, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

75. Wayne Bank failed to ensure that the vendor to whom Defendant gave its customers' PII properly implemented basic data security practices widely known throughout the industry.

76. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patient Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

77. Defendant was at all times fully aware of its obligations to protect the PII of its current and former customers. Defendant was also aware of the significant repercussions that would result from their failure to do so.

F. Defendant Fails to Comply with Industry Standards

78. As noted above, experts studying cyber security routinely identify entities in possession of PII as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

79. Several best practices have been identified that a minimum should be implemented by entities in possession of PII, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

80. Other best cybersecurity practices that are standard for entities include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

81. Defendant failed to ensure that its vendor, MOVEit, to whom it gave Plaintiff's and the proposed Class Members' PII, met the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

82. These foregoing frameworks are existing and applicable industry standards for an company's obligations to provide adequate data security for its customers. Upon information and belief, Defendant failed to ensure that its vendor complied with at least one– or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

V. CLASS ACTION ALLEGATIONS

83. Plaintiff brings this class action under Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), individually and on behalf of all members of the following nationwide class ("Nationwide Class" or "Class"):

> **All individuals who were customers of Defendant and/or who entrusted their PII to Defendant and whose PII was compromised in the Data Breach and MOVEit vulnerability.**

84. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

85. Plaintiff reserves the right to amend the class definition.

86. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of their claims on class-wide bases using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

87. **Numerosity**. The Class Members are so numerous that joinder of all Class Members is impracticable.

88. **Commonality and Predominance**. Plaintiff and the Class's claims raise predominantly common fact and legal questions, which predominate over any questions affecting individual Class members, that a class wide proceeding can answer for all Class members. Indeed, it will be necessary to answer the following questions:

a. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's PII, including exercising reasonable care in ensuring that its vendors to whom it gave PII adequately safeguarded customers' PII;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach and failed to ensure that its vendors implemented and maintained reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant were negligent in maintaining, protecting, and securing PII including whether Defendant was negligent in ensuring that its vendors maintained, protected, and secured PII;

d. Whether Defendant breached contractual promises to safeguard Plaintiff's and the Class's PII;

e. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

f. Whether Defendant's Data Breach Notice was reasonable;

g. Whether the Data Breach caused Plaintiff's and the Class's injuries;

h. What the proper damages measure is; and

i. Whether Plaintiff and the Class are entitled to damages, treble damages, or injunctive relief.

89. **Typicality**. Plaintiff's claims are typical of Class member's claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

90. **Adequacy**. Plaintiff will fairly and adequately protect the proposed Class's common interests. Their interests do not conflict with Class members' interests. They have also

retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

91. **Superiority.** A class action is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class members are relatively small compared to the burden and expense that would be entailed by individual litigation of their claims against Defendant. It would thus be virtually impossible for the Class members, on an individual basis, to obtain effective redress for the wrongs done to them. Individualized litigation would create the danger of inconsistent or contradictory judgments arising from the same set of facts and would also increase the delay and expense to all parties and the courts. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, ensures economies of scale and comprehensive supervision by a single court, and presents no unusual management difficulties under the circumstances here.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiff and the Class)

92. Plaintiff realleges all previous paragraphs as if fully set forth below.

93. Plaintiff and Class Members entrusted their PII to Defendant. Defendant owed to Plaintiff and other Class Members a duty to exercise reasonable care in handling and using the PII in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

94. Defendant owed Plaintiff and other Class Members a duty to ensure that its vendor implemented industry-standard security procedures sufficient to reasonably protect the PII from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detected attempts at unauthorized access.

95. Defendant owed a duty of care to Plaintiff and Class Members because it was

foreseeable that Defendant's failure to adequately safeguard their PII in accordance with state-of-the-art industry standards concerning data security, and failing to ensure that its vendor adequately safeguarded their PII in accordance with state-of-the-art industry standards concerning data security, would result in the compromise of that PII—just like the Data Breach that ultimately came to pass.

96. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff' and Class Members' PII by disclosing and providing access to this information to third parties that did not adequately protect this PII and by failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

97. Defendant owed to Plaintiff and Class Members a duty to notify them within a reasonable timeframe of any breach to the security of their PII. Defendant also owed a duty to timely and accurately disclose to Plaintiff and Class Members the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and Class Members to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

98. Defendant owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff' and Class Members' personal information and PII.

99. Under the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff and Class Members' PII and to ensure its vendors provided the same security practices.

100. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect consumers' PII. The FTC publications

and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff and the Class Members' sensitive PII.

101. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

102. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant's vendor, MOVEit holds vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendant's vendors' databases containing the PII—whether by malware or otherwise.

103. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiff and Class Members' and the importance of exercising reasonable care in handling it.

104. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII of Plaintiff and Class Members which actually and proximately caused the Data Breach and Plaintiff and Class Members' injury. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and Class Members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff and Class Members' injuries-in-fact. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and Class Members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

105. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and Class Members actual,

tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

SECOND CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

106. Plaintiff and Class Members incorporate the above allegations as if fully set forth herein.

107. Plaintiff and Class Members were required to provide their PII to Defendant as a condition of receiving services provided by Defendant. Plaintiff and Class Members provided their PII to Defendant or its third-party agents in exchange for Defendant's services.

108. In turn, and through internal policies, Defendant agreed they would not disclose the PII it collects to unauthorized persons. Defendant also promised to safeguard PII.

109. Plaintiff and the Class Members accepted Defendant's offers by disclosing their PII to Defendant or its third-party agents in exchange for financial services.

110. Implicit in the parties' agreement was that Defendant would provide Plaintiff and Class Members with prompt and adequate notice of all unauthorized access and/or theft of their PII.

111. Plaintiff and the Class Members would not have entrusted their PII to Defendant or its third-party agents in the absence of such agreement with Defendant.

112. Defendant materially breached the contract(s) it had entered with Plaintiff and Class Members by failing to safeguard such information and failing to notify them promptly of the intrusion into its computer systems that compromised such information. Defendant further breached the implied contracts with Plaintiff and Class Members by:

a. Failing to properly safeguard and protect Plaintiff and Class Members' PII,

including ensuring its vendors to whom it gave PII adequately safeguarded customers' PII;

b. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement; and

c. Failing to ensure the confidentiality and integrity of electronic PII that Defendant created, received, maintained, and transmitted.

113. The damages sustained by Plaintiff and Class Members as described above were the direct and proximate result of Defendant's material breaches of their agreement(s).

114. Plaintiff and Class Members have performed as required under the relevant agreements, or such performance was waived by the conduct of Defendant.

115. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose upon each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

116. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

117. Defendant failed to advise Plaintiff and Class Members of the Data Breach promptly and sufficiently.

118. In these and other ways, Defendant violated its duty of good faith and fair dealing.

119. Plaintiff and Class Members have sustained damages because of Defendant's breaches of its agreement, including breaches thereof through violations of the covenant of good faith and fair dealing.

THIRD CAUSE OF ACTION

Unjust Enrichment
(On Behalf of Plaintiff and the Class)

120. Plaintiff and Class Members incorporate the above allegations as if fully set forth herein.

121. This claim is pleaded in the alternative to the breach of implied contractual duty claim.

122. Plaintiff and Class Members conferred a benefit upon Defendant. After all, Defendant benefitted from using their PII to facilitate its business as a financial institution.

123. Defendant itself admits that it collects customers personal information to "develop individualized Online Banking experience[s]" and to "allow the Bank to understand customer preferences in order to present new products and services which are suitable to personal interests."[18]

124. Defendant appreciated or had knowledge of the benefits conferred upon them by Plaintiff and Class Members. And simply put, Defendant benefited from the receipt of Plaintiff and Class Members' PII, as this was used to provide its services.

125. Under principals of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff and the proposed Class's services and their PII because Defendant failed to adequately protect their PII.

126. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds received by it because of its misconduct and Data Breach.

FOURTH CAUSE OF ACTION
INVASION OF PRIVACY
(On Behalf of Plaintiff and the Class)

[18] Ex. C.

127. Plaintiff incorporates all previous paragraphs as if fully set forth below.

128. Defendant publicized private details and facts not generally known to the public, not publicly available, and not of legitimate public concern about Plaintiff and the Class Members by disclosing and exposing Plaintiff's and the Class Members' Personal Information to enough people that it is reasonably likely those facts have and/or will become known to the public at large, including, without limitation, on the dark web and elsewhere. The disclosure of customers' names, Social Security numbers, and financial information, is particularly harmful and would be offensive to a reasonable person of ordinary sensibilities.

129. Defendant has a special relationship with Plaintiff and the Class Members and Defendant's disclosure of PII is certain to embarrass them and offend their dignity. Defendant should appreciate that the cyber-criminals who stole the Personal Information would fraudulently misuse that Personal Information, and further sell and disclose the data, just as they are doing. That the original disclosure is devastating to the Plaintiff and the Class Members, even though it originally may have only been disclosed to one person or a limited number of cyber-criminals, does not render it any less a disclosure to the public-at-large considering that said non-public information is now made public, and cannot be secured again.

130. Plaintiff's and the Class Members' PII was publicly disclosed by Defendant in the Data Breach with reckless disregard for the reasonable offensiveness of the disclosure. Such disclosure is highly offensive and would be to any person of ordinary sensibilities. Defendant knew or should have known that Plaintiff's and the Class Members' PII is not a matter of legitimate public concern.

131. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been injured and are entitled to damages, as set forth herein.

VI. PRAYER FOR RELIEF

Plaintiff and Class Members demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing her counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PII;

E. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

VII. DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury as to all claims of the Complaint so triable.

RESPECTFULLY SUBMITTED AND DATED this 12th day of February, 2024.

BY: */S/ Patrick Howard*

Patrick Howard (PA ID #88572)
SALTZ, MONGELUZZI, & BENDESKY, P.C.
1650 Market Street, 52nd Floor
Philadelphia, PA 19103
Tel: (215) 496-8282
Fax: (215) 496-0999
phoward@smbb.com

Samuel J. Strauss (Pro Hac Vice forthcoming)
Raina Borelli (Pro Hac Vice forthcoming)
TURKE & STRAUSS LLP
613 Williamson St., Suite 201
Madison, WI 53703
Telephone: (608) 237-1775
Facsimile: (608) 509-4423
sam@turkestrauss.com
raina@turkestrauss.com

Lynn A. Toops (*Pro Hac Vice* forthcoming
Amina A. Thomas (*Pro Hac Vice* forthcoming)
COHEN & MALAD, LLP
One Indiana Square, Suite 1400
Indianapolis, Indiana 46204
(317) 636-6481
ltoops@cohenandmalad.com
athomas@cohenandmalad.com

J. Gerard Stranch, IV (*Pro Hac Vice* forthcoming)
Andrew E. Mize (*Pro Hac Vice* forthcoming)
STRANCH, JENNINGS & GARVEY, PLLC
The Freedom Center
223 Rosa L. Parks Avenue, Suite 200
Nashville, Tennessee 37203
(615) 254-8801
(615) 255-5419 (facsimile)
gstranch@stranchlaw.com
amize@stranchlaw.com

Counsel for Plaintiff and the Proposed Class